

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-175402

(43)Date of publication of application : 02.07.1999

(51)Int.Cl.

G06F 12/14
B42D 15/10
G06K 17/00
G06K 19/073
G06K 19/07

(21)Application number : 09-340382

(71)Applicant : FUJITSU LTD

(22)Date of filing : 10.12.1997

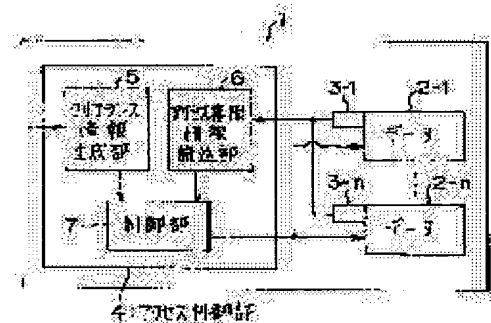
(72)Inventor : ASO IZUMI
TSUBURA SHUICHI

(54) CARD TYPE STORAGE MEDIUM AND ACCESS CONTROL METHOD FOR THE SAME AND COMPUTER READABLE RECORDING MEDIUM FOR RECORDING ACCESS CONTROL PROGRAM FOR CARD TYPE STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To accurately attain the management and operation of a security system while simplifying the setting and charging work of access authority in a card type storage medium such as an IC card.

SOLUTION: This card type storage medium 1 is provided with storage parts 2-1 to 2-n for storing data and an access control part 4 for controlling access from an access subject to data. The access control part 4 is constituted so as to be provided with an access subject identification information generating part 5 for generating access subject identification information for identifying the access subject, an access authority information reading part 6 for reading access authority information 3-1 to 3-n set corresponding to data being the destination of an access request from the access subject and a control part 7 for obtaining the access authority from the access subject identification information and the access authority information 3-1 to 3-n and controlling the access from the access subject to the data based on the obtained access authority.



LEGAL STATUS

[Date of request for examination] 28.03.2001

[Date of sending the examiner's decision of rejection] 06.09.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision
of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-175402

(43) 公開日 平成11年(1999) 7月2日

(51) Int.Cl.⁸

識別記号

F I

G 0 6 F 12/14

3 1 0

G 0 6 F 12/14

3 1 0 K

B 4 2 D 15/10

5 2 1

B 4 2 D 15/10

5 2 1

G 0 6 K 17/00

G 0 6 K 17/00

E

19/073

19/00

P

19/07

N

審査請求 未請求 請求項の数14 O L (全 24 頁)

(21) 出願番号

特願平9-340382

(22) 出願日

平成9年(1997)12月10日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 麻生 泉

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72) 発明者 堀良 修一

群馬県前橋市間屋町1丁目8番3号 株式
会社富士通ターミナルシステムズ内

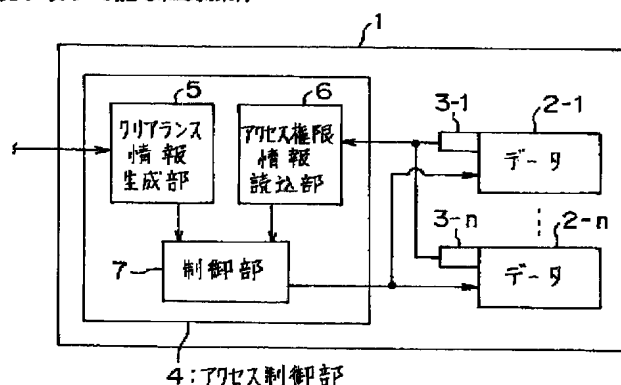
(74) 代理人 弁理士 真田 有

(54) 【発明の名称】 カード型記憶媒体及びカード型記憶媒体のアクセス制御方法並びにカード型記憶媒体用アクセス制御プログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 ICカードのようなカード型記憶媒体において、アクセス権限の設定、変更作業を簡素化しながら、セキュリティシステムの管理、運営を確実にこなえるようにする。

【解決手段】 データを格納する記憶部2-1~2-nと、アクセス主体からデータへのアクセスを制御するアクセス制御部4とをそなえたカード型記憶媒体1であって、アクセス制御部4が、アクセス主体を識別するためのアクセス主体識別情報を生成するアクセス主体識別情報生成部5と、アクセス主体からのアクセス要求先となるデータに対応して設定されたアクセス権限情報3-1~3-nを読み込むアクセス権限情報読込部6と、上記アクセス主体識別情報及びアクセス権限情報3-1~3-nからアクセス権限を求め、求められたアクセス権限に基づいて、アクセス主体からのデータへのアクセスを制御する制御部7とをそなえるように構成する。



(2)

【特許請求の範囲】

【請求項1】 アクセス対象となるデータを格納する記憶部と、アクセス主体から該データへのアクセスを制御するアクセス制御部とをそなえたカード型記憶媒体であって、

該アクセス制御部が、

該アクセス主体を識別するためのアクセス主体識別情報を生成するアクセス主体識別情報生成部と、

該アクセス主体からのアクセス要求先となる該データに対応して設定されたアクセス権限を求めるためのアクセス権限情報を読み込むアクセス権限情報読込部と、

上記アクセス主体識別情報及びアクセス権限情報から該アクセス主体識別情報に対応したアクセス権限を求め、求められた該アクセス権限に基づいて、該アクセス主体からの該データへのアクセスを制御する制御部とをそなえて構成されることを特徴とする、カード型記憶媒体。

【請求項2】 該アクセス主体識別情報が、少なくとも2つ以上のアクセスするための条件に関する情報により構成されることを特徴とする、請求項1記載のカード型記憶媒体。

【請求項3】 該アクセス主体識別情報が、オペレータを照合するための照合用アクセス主体識別情報と、アプリケーションを認証するための認証用アクセス主体識別情報とにより構成されることを特徴とする、請求項1記載のカード型記憶媒体。

【請求項4】 該照合用アクセス主体識別情報がオペレータの身分を示すアクセス主体照合情報に対応するものであるとともに、該認証用アクセス主体識別情報がアプリケーションを識別するためのアクセス主体認証情報に対応するものであることを特徴とする、請求項3記載のカード型記憶媒体。

【請求項5】 上記照合用アクセス主体識別情報及び認証用アクセス主体識別情報が、それぞれ少なくとも1つ以上のカテゴリ情報と階層をもつレベル情報とのマトリックスで表現されたことを特徴とする、請求項3記載のカード型記憶媒体。

【請求項6】 該アクセス権限情報が、該マトリックスの各要素毎に上記照合用アクセス主体識別情報及び認証用アクセス主体識別情報を条件として決定されるアクセス権限要素と、該アクセス権限要素を用いた演算関数とにより構成されることを特徴とする、請求項5記載のカード型記憶媒体。

【請求項7】 該アクセス主体識別情報生成部が、オペレータを照合するためのデフォルトの照合用アクセス主体識別情報、アプリケーションを認証するためのデフォルトの認証用アクセス主体識別情報、オペレータの身分を示す参照用のアクセス主体照合情報、アプリケーションを識別するための参照用のアクセス主体認証情報、該参照用のアクセス主体照合情報に対応したオペレータを照合するための照合用アクセス主体識別情報を発生する

2

とともに該参照用のアクセス主体認証情報に対応したアプリケーションを認証するための認証用アクセス主体識別情報を発生するためのアクセス主体識別情報発生情報及び発生した該照合用アクセス主体識別情報を該デフォルトの照合用アクセス主体識別情報に反映させるとともに発生した該認証用アクセス主体識別情報を該デフォルトの認証用アクセス主体識別情報に反映させるための演算関数を保持することを特徴とする、請求項1記載のカード型記憶媒体。

【請求項8】 該アクセス主体から該データにアクセスするための論理チャネルを複数そなえ、該アクセス制御部が、該アクセス主体から該データへのアクセスを該論理チャネル毎に独立して制御することを特徴とする、請求項1記載のカード型記憶媒体。

【請求項9】 該アクセス制御部が、該論理チャネル毎に該アクセス主体識別情報を生成することを特徴とする、請求項8記載のカード型記憶媒体。

【請求項10】 該アクセス制御部における動作を監査した内容である監査ログを保持することを特徴とする、請求項1記載のカード型記憶媒体。

【請求項11】 アクセス対象となるデータを格納する記憶部をそなえたカード型記憶媒体において、アクセス主体から該データへのアクセスを制御するためのカード型記憶媒体のアクセス制御方法であって、

該アクセス主体を識別するためのアクセス主体識別情報を生成するアクセス主体識別情報生成ステップと、

該アクセス主体からのアクセス要求先となる該データに対応して設定されたアクセス権限を求めるためのアクセス権限情報を読み込むアクセス権限情報読込ステップと、

上記アクセス主体識別情報及びアクセス権限情報から該アクセス主体識別情報に対応したアクセス権限を求め、求められた該アクセス権限に基づいて、該アクセス主体からの該データへのアクセスを制御する制御ステップとをそなえて構成されることを特徴とする、カード型記憶媒体のアクセス制御方法。

【請求項12】 アクセス主体識別情報生成ステップが、該アクセス主体からオペレータの身分を示すアクセス主体照合情報及びアプリケーションを識別するためのアクセス主体認証情報が入力されると、入力された上記アクセス主体照合情報及びアクセス主体認証情報と参照用のアクセス主体照合情報及び参照用のアクセス主体認証情報とを比較し、一致した場合には、上記参照用のアクセス主体照合情報及び参照用のアクセス主体認証情報に対応したオペレータを照合するための照合用アクセス主体識別情報及びアプリケーションを認証するための認証用アクセス主体識別情報を発生し、発生した上記照合用アクセス主体識別情報及び認証用アクセス主体識別情報をオペレータを照合するためのデフォルトの照合用アクセス主体識別情報及びアプリケーションを認証するた

(3)

3

めのデフォルトの認証用アクセス主体識別情報に反映させることを特徴とする、請求項1記載のカード型記憶媒体のアクセス制御方法。

【請求項13】 該アクセス主体識別情報が、オペレータを照合するための照合用アクセス主体識別情報と、アプリケーションを認証するための認証用アクセス主体識別情報とにより構成され、

該制御ステップが、上記照合用アクセス主体識別情報及び認証用アクセス主体識別情報を条件としてアクセス権限要素を決定し、該アクセス権限要素を用いた演算により、該アクセス主体識別情報に対応したアクセス権限を

求めることを特徴とする、請求項1記載のカード型記憶媒体のアクセス制御方法。

【請求項14】 アクセス対象となるデータを格納する記憶部をそなえたカード型記憶媒体において、アクセス主体から該データへのアクセスをコンピュータにより制御するためのカード型記憶媒体用アクセス制御プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

該カード型記憶媒体用アクセス制御プログラムが、該アクセス主体を識別するためのアクセス主体識別情報を生成するアクセス主体識別情報生成部、

該アクセス主体からのアクセス要求先となる該データに対応して設定されたアクセス権限を求めるためのアクセス権限情報を読み込むアクセス権限情報読込部、および、

上記アクセス主体識別情報及びアクセス権限情報から該アクセス主体識別情報に対応したアクセス権限を求め、求められたアクセス権限に基づいて、該アクセス主体からの該データへのアクセスを制御する制御部として、該コンピュータを機能させることを特徴とする、カード型記憶媒体用アクセス制御プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】（目次）

発明の属する技術分野

従来の技術（図46、図47）

発明が解決しようとする課題

課題を解決するための手段

発明の実施の形態

・（a）一実施形態の説明（図1～図5、図7～図45）

・（b）その他（図6）

発明の効果

【0002】

【発明の属する技術分野】本発明は、例えば電子マネー可搬媒体、クレジットカード、IDカード、自治体カード等として用いられるICカードのようなカード型記憶媒体に関し、更にはこのようなカード型記憶媒体のアクセス制御方法並びにカード型記憶媒体用アクセス制御プ

4

ログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0003】近年、ICカードの利用分野の拡大とともに、セキュリティが求められる重要な情報、例えば、電子マネー情報、クレジットカード情報、医療カルテ情報等がICカードの中に格納されるようになってきている。従って、ICカードでは、これらの情報を安全に蓄えることが要求されている。このため、国際規格（ISO7816）に則ったコマンドを用いてアクセス制御を行なう中で、セキュリティを高める必要がある。

【0004】

【従来の技術】従来より、カード型記憶媒体にてアクセス制御を行なうための技術としては、特開昭60-160491号公報（ICカード）、特開昭60-205688号公報（携帯可能媒体）、特開昭60-205689号公報（携帯可能媒体）、特開昭60-205690号公報（携帯可能媒体）、特開昭60-207939号公報（電子装置の記録方式）等に記載された技術が、カード型記憶媒体のセキュリティを高める手段として有効であると考えられてきた。

【0005】例えば、特開昭60-160491号公報（ICカード）に記載された技術について、図46

（a）、図46（b）及び図47を用いて説明する。図46（a）に示すように、ICカード100は、アクセス対象となるデータを格納するファイル101-1、101-2をそなえており、ファイル101-1、101-2には、それぞれアクセス権限情報（セキュリティ管理情報）102-1、102-2が付与されている。

【0006】また、クライアント103Aには暗証番号（pin）“a”が与えられており、クライアント103Bには暗証番号“a、c”が与えられており、クライアント103Cには暗証番号“a、b”が与えられている。ここで、ファイル101-1、101-2に付与されるアクセス権限情報102-1、102-2はともに“a、b”であるため、暗証番号“a、b”をもっているクライアント103Cのみがファイル101-1、101-2をリードすることができる。

【0007】このような前提のもとで、クライアント103Aに、ファイル101-1へのリード権を新たに設定する場合について考える。ただし、クライアント103Aにはファイル101-2へのアクセスは認められず、また、クライアント103Bにはファイル101-1へのアクセスは認められない。さらに、クライアント103Cへの影響は避けるものとする。

【0008】この場合には、図46（b）に示すように、クライアント103Aに更に暗証番号“d”を与えて、クライアント103Aのもつ暗証番号を“a、d”とするとともに、ファイル101-1のアクセス権限情報102-1の設定を、符号102-1'に示すように変更すれば、クライアント103Aに、ファイル101

50

(4)

5

ー1へのリード権を新たに設定することができる。

【0009】さらに、この後に、暗証番号“b, c”をもつクライアント103Dに対して、ファイル101-1へのリード権を新たに設定する場合について考える。この場合には、図47に示すように、クライアント103Dに更に暗証番号“d”を与えて、クライアント103Dのもつ暗証番号を“b, c, d”とするとともに、ファイル101-1のアクセス権限情報102-1'の設定を、符号102-1"に示すように変更すれば、クライアント103Dにも、ファイル101-1へのリード権を新たに設定することができる。

【0010】なお、図46(b)及び図47においては、ファイル101-2及びアクセス権限情報102-2の図示を省略している。

【0011】

【発明が解決しようとする課題】しかしながら、上述したカード型記憶媒体におけるアクセス制御方法においては、アクセス権限の設定、変更方法やセキュリティシステムの使用、維持管理方法がわかりにくく、セキュリティシステムの設計者にとって、アクセス権限の設定、変更作業やセキュリティシステムの使用、維持管理作業がかなり煩雑なものとなるという課題がある。

【0012】つまり、クライアント103A~103Dのアクセス権限を拡大したり縮小する場合には、ファイル101-1, 101-2に付与されているアクセス権限情報102-1, 102-2の見直しを行わなければならない、アクセス権限の設定、変更作業がシステム全体に影響を及ぼすことになる。即ち、このようにセキュリティシステムを定義した後のアクセス権限の変更は、セキュリティシステムの全体を見回してから行なうことが必要となり、アクセス権限の設定、変更作業がかなり煩雑なものとなるのである。

【0013】なお、前述した他の公報に記載された技術においても同様の課題を有している。さらに、電子マネー情報、クレジットカード情報、自治体情報等を1つのカード型記憶媒体に格納するような多目的利用を考えた場合には、セキュリティシステムの運用上、1か所でセキュリティの管理が行なえ、かつ用途間で情報の独立が保たれるようにすることが必要とされている。

【0014】本発明は、このような課題に鑑み創案されたもので、多目的利用を考えた場合であっても、アクセス権限の設定、変更作業を簡素化しながら、セキュリティシステムの管理、運営を確実に行なえるようにした、カード型記憶媒体及びカード型記憶媒体のアクセス制御方法を提供することを目的とするとともに、更には、アクセス主体からのデータアクセスを制御するためのカード型記憶媒体用アクセス制御プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0015】

6

【課題を解決するための手段】このため、本発明のカード型記憶媒体は、アクセス対象となるデータを格納する記憶部と、アクセス主体からデータへのアクセスを制御するアクセス制御部とをそなえたカード型記憶媒体であって、アクセス制御部が、アクセス主体を識別するためのアクセス主体識別情報を生成するアクセス主体識別情報生成部と、アクセス主体からのアクセス要求先となるデータに対応して設定されたアクセス権限を求めるためのアクセス権限情報を読み込むアクセス権限情報読込部と、上記アクセス主体識別情報及びアクセス権限情報からアクセス主体識別情報に対応したアクセス権限を求め、求められたアクセス権限に基づいて、アクセス主体からのデータへのアクセスを制御する制御部とをそなえて構成されることを特徴としている（請求項1）。

【0016】また、本発明のカード型記憶媒体は、請求項1記載のカード型記憶媒体において、アクセス主体識別情報が、少なくとも2つ以上のアクセスするための条件に関する情報により構成されることを特徴としている（請求項2）。さらに、本発明のカード型記憶媒体は、請求項1記載のカード型記憶媒体において、アクセス主体識別情報が、オペレータを照合するための照合用アクセス主体識別情報と、アプリケーションを認証するための認証用アクセス主体識別情報とにより構成されることを特徴としている（請求項3）。

【0017】また、本発明のカード型記憶媒体は、請求項3記載のカード型記憶媒体において、照合用アクセス主体識別情報がオペレータの身分を示すアクセス主体照合情報に対応するものであるとともに、認証用アクセス主体識別情報がアプリケーションを識別するためのアクセス主体認証情報に対応するものであることを特徴としている（請求項4）。

【0018】さらに、本発明のカード型記憶媒体は、請求項3記載のカード型記憶媒体において、上記照合用アクセス主体識別情報及び認証用アクセス主体識別情報が、それぞれ少なくとも1つ以上のカテゴリ情報と階層をもつレベル情報とのマトリックスで表現されたことを特徴としている（請求項5）。また、本発明のカード型記憶媒体は、請求項5記載のカード型記憶媒体において、アクセス権限情報が、マトリックスの各要素毎に上記照合用アクセス主体識別情報及び認証用アクセス主体識別情報を条件として決定されるアクセス権限要素と、アクセス権限要素を用いた演算関数とにより構成されることを特徴としている（請求項6）。

【0019】さらに、本発明のカード型記憶媒体は、請求項1記載のカード型記憶媒体において、アクセス主体識別情報生成部が、オペレータを照合するためのデフォルトの照合用アクセス主体識別情報、アプリケーションを認証するためのデフォルトの認証用アクセス主体識別情報、オペレータの身分を示す参照用のアクセス主体照合情報、アプリケーションを識別するための参照用のア

50

(5)

7
 クセス主体認証情報、参照用のアクセス主体照合情報に対応したオペレータを照合するための照合用アクセス主体識別情報を発生するとともに参照用のアクセス主体認証情報に対応したアプリケーションを認証するための認証用アクセス主体識別情報を発生するためのアクセス主体識別情報発生情報及び発生した照合用アクセス主体識別情報をデフォルトの照合用アクセス主体識別情報に反映させるとともに発生した認証用アクセス主体識別情報をデフォルトの認証用アクセス主体識別情報に反映させるための演算関数を保持することを特徴としている（請求項7）。

【0020】また、本発明のカード型記憶媒体は、請求項1記載のカード型記憶媒体において、アクセス主体からデータにアクセスするための論理チャネルを複数そなえ、アクセス制御部が、アクセス主体からデータへのアクセスを論理チャネル毎に独立して制御することを特徴としている（請求項8）。さらに、本発明のカード型記憶媒体は、請求項8記載のカード型記憶媒体において、アクセス制御部が、論理チャネル毎にアクセス主体識別情報を生成することを特徴としている（請求項9）。

【0021】また、本発明のカード型記憶媒体は、請求項1記載のカード型記憶媒体において、アクセス制御部における動作を監査した内容である監査ログを保持することを特徴としている（請求項10）。ところで、本発明のカード型記憶媒体のアクセス制御方法は、アクセス対象となるデータを格納する記憶部をそなえたカード型記憶媒体において、アクセス主体からデータへのアクセスを制御するためのカード型記憶媒体のアクセス制御方法であって、アクセス主体を識別するためのアクセス主体識別情報を生成するアクセス主体識別情報生成ステップと、アクセス主体からのアクセス要求先となるデータに対応して設定されたアクセス権限を求めるためのアクセス権限情報を読み込むアクセス権限情報読込ステップと、上記アクセス主体識別情報及びアクセス権限情報からアクセス主体識別情報に対応したアクセス権限を求め、求められたアクセス権限に基づいて、アクセス主体からのデータへのアクセスを制御する制御ステップとをそなえて構成されることを特徴としている（請求項11）。

【0022】また、本発明のカード型記憶媒体のアクセス制御方法は、請求項11記載のカード型記憶媒体のアクセス制御方法において、アクセス主体識別情報生成ステップが、アクセス主体からオペレータの身分を示すアクセス主体照合情報及びアプリケーションを識別するためのアクセス主体認証情報が入力されると、入力された上記アクセス主体照合情報及びアクセス主体認証情報と参照用のアクセス主体照合情報及び参照用のアクセス主体認証情報とを比較し、一致した場合には、上記参照用のアクセス主体照合情報及び参照用のアクセス主体認証情報に対応したオペレータを照合するための照合用アク

8

セス主体識別情報及びアプリケーションを認証するための認証用アクセス主体識別情報を発生し、発生した上記照合用アクセス主体識別情報及び認証用アクセス主体識別情報をオペレータを照合するためのデフォルトの照合用アクセス主体識別情報及びアプリケーションを認証するためのデフォルトの認証用アクセス主体識別情報に反映させることを特徴としている（請求項12）。

【0023】さらに、本発明のカード型記憶媒体のアクセス制御方法は、請求項11記載のカード型記憶媒体のアクセス制御方法において、アクセス主体識別情報が、オペレータを照合するための照合用アクセス主体識別情報と、アプリケーションを認証するための認証用アクセス主体識別情報とにより構成され、制御ステップが、上記照合用アクセス主体識別情報及び認証用アクセス主体識別情報を条件としてアクセス権限要素を決定し、アクセス権限要素を用いた演算により、アクセス主体識別情報に対応したアクセス権限を求めることを特徴としている（請求項13）。

【0024】ところで、本発明のカード型記憶媒体用アクセス制御プログラムを記録したコンピュータ読み取り可能な記録媒体は、アクセス対象となるデータを格納する記憶部をそなえたカード型記憶媒体において、アクセス主体からデータへのアクセスをコンピュータにより制御するためのカード型記憶媒体用アクセス制御プログラムを記録したコンピュータ読み取り可能な記録媒体であって、カード型記憶媒体用アクセス制御プログラムが、アクセス主体を識別するためのアクセス主体識別情報を生成するアクセス主体識別情報生成部、アクセス主体からのアクセス要求先となるデータに対応して設定されたアクセス権限を求めるためのアクセス権限情報を読み込むアクセス権限情報読込部、および、上記アクセス主体識別情報及びアクセス権限情報からアクセス主体識別情報に対応したアクセス権限を求め、求められたアクセス権限に基づいて、アクセス主体からのデータへのアクセスを制御する制御部として、コンピュータを機能させることを特徴としている（請求項14）。

【0025】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。

（a）一実施形態の説明

図1～図3は本発明の一実施形態にかかるカード型記憶媒体の構成を示す機能ブロック図であり、この図1～図3に示すカード型記憶媒体1は、例えば電子マネー可搬媒体、クレジットカード、IDカード、自治体カード等として用いられるICカードであって、アクセス対象となるデータを格納するファイル（記憶部）2-i（i=1～n, n:任意の自然数）、アクセス主体〔以下では、カード型記憶媒体1の所有者、この所有者がアクセスの際に用いる端末、実際にアクセスを行なうアプリケーション（クライアントアプリケーション）を総称して

(6)

9

アクセス主体という。)からデータへのアクセスを制御するアクセス制御部4とをそなえて構成されている。

【0026】ここで、ファイル2-iにおけるデータには、それぞれ、アクセス主体がそのデータにアクセスすることができるか否かを示すアクセス権限を求めるためのアクセス権限情報3-i ($i=1\sim n$, n :任意の自然数)が付与されている。また、アクセス制御部4は、図1に示すように、アクセス主体を識別するためのクリアランス情報(アクセス主体識別情報;図2に符号9で示す)を生成するクリアランス情報生成部(アクセス主体識別情報生成部)5と、アクセス主体からのアクセス要求先となるデータに対応して設定されたアクセス権限情報3-iを読み込むアクセス権限情報読込部6と、上記クリアランス情報9及びアクセス権限情報3-iからアクセス主体識別情報3-iに対応したアクセス権限を求め、求められたアクセス権限に基づいて、アクセス主体からのデータへのアクセスを制御する制御部7とをそなえて構成されている。

【0027】さらに、カード型記憶媒体1は、図2、図3に示すように、実際にアクセスを行なうクライアントアプリケーション12をそなえており、このクライアントアプリケーション12とアクセス制御部4との間には論理チャネル13が設けられている。また、カード型記憶媒体1は、図2に示すように、アクセス制御部4における動作を監査した内容である監査ログ8を保持するように構成されている。なお、監査ログの一例を図7に示す。この監査ログは、監査ログ用のIEF[内部EF(Elementary File)];後述にて用いる図19等を参照)に格納されている。ここで、IEFは順レコード構造となっており、コマンド受信/処理順にシーケンシャルに格納されている。

【0028】なお、符号11はカード型記憶媒体1内のデータを用いた各種の処理を行なう端末であり、符号10はカード型記憶媒体1が挿入接続され、端末11からの読み書き命令を伝達するカード接続装置である。また、クライアントアプリケーション12は、カード接続装置10、端末11内にあってもよい。図2では、カード型記憶媒体1、カード接続装置10、端末11の全てがクライアントアプリケーション12をそなえているように記載されている。

【0029】さらに、カード型記憶媒体1は、図3に示すように、カード接続装置10とのインタフェース部としての通信制御部14をそなえている。なお、この図3については、後述にて詳細に説明する。ここで、前述したクリアランス情報9及びアクセス権限情報3-iについて説明する。

【0030】クリアランス情報9は、アクセス主体を識別するための情報であるが、本実施形態にかかるカード型記憶媒体1においては、クリアランス情報9は、少なくとも2つ以上のアクセスするための条件に関する情報

10

により構成されている。具体的には、クリアランス情報9は、図5に示すように、照合用クリアランス情報9Aと認証用クリアランス情報9Bとから構成されている。

【0031】ここで、照合用クリアランス情報9Aは、オペレータがカード型記憶媒体1の所有者であるかを確認するために、オペレータを照合するための情報であり、オペレータの身分を示すアクセス主体照合情報[暗証番号(pin)]に対応するものである。また、認証用クリアランス情報9Bは、アクセス可能な端末11を使用したアクセスであるかを確認するために、クライアントアプリケーション12を認証するための情報であり、クライアントアプリケーション12を識別するためのアクセス主体認証情報(端末11から送信される認証キー情報)に対応するものである。

【0032】そして、照合用クリアランス情報9A及び認証用クリアランス情報9Bは、図10(a)、図10(b)に示すように、それぞれ少なくとも1つ以上のカテゴリ情報と階層をもつレベル情報とのマトリックスで表現されている。なお、図10(a)、図10(b)では、カテゴリ情報の一例として企業内の各部署名(人事、経理、総務、開発、購買)が用いられるとともに、階層をもつレベル情報の一例として企業内の役職名(部長、担当部長、課長、一般職)が用いられている。また、図10(c)では、照合用クリアランス情報9A及び認証用クリアランス情報9Bをまとめて表現した様子を仮想的に示している。

【0033】そして、本実施形態においては、このような照合用クリアランス情報9A及び認証用クリアランス情報9Bを生成するために、クリアランス情報生成部5が、デフォルトの照合用クリアランス情報、デフォルトの認証用クリアランス情報、参照用の暗証番号(参照用のアクセス主体照合情報)、参照用の認証キー情報(参照用のアクセス主体認証情報)、参照用の暗証番号に対応した照合用クリアランス情報を発生するとともに参照用の認証キー情報に対応した認証用クリアランス情報を発生するためのアクセス主体識別情報発生情報及び発生した照合用クリアランス情報をデフォルトの照合用クリアランス情報に反映させるとともに発生した認証用クリアランス情報をデフォルトの認証用クリアランス情報に反映させるための演算関数を保持している。なお、これらの情報を用いた照合用クリアランス情報9A及び認証用クリアランス情報9Bを生成については後述する。

【0034】また、アクセス権限情報3-iは、アクセス主体のアクセス権限を求めるための情報であるが、本実施形態にかかるカード型記憶媒体1においては、アクセス権限情報3-iは、図11に示すように、マトリックスの各要素毎に照合用クリアランス情報9A及び認証用クリアランス情報9Bを条件として決定されるアクセス権限要素(図11の符号Q参照)と、これらのアクセス権限要素を用いた演算関数(図11の式(1)参照)

50

(7)

11

とにより構成されている。なお、このアクセス権限情報3-iは、セキュリティシステムの設計者により、適宜設定される。

【0035】なお、実際には、本実施形態にかかるカード型記憶媒体1において、上述したアクセス制御部4に相当する機能（即ち、クリアランス情報生成部5、アクセス権限情報読込部6及び制御部7に相当する機能）は、カード型記憶媒体1内のROMや図2に示す端末11等のようなコンピュータにおけるディスク装置等の記録媒体（ともに図示せず）に記録されたプログラム（以下、カード型記憶媒体用アクセス制御プログラムという）を、カード型記憶媒体1内又は図2に示す端末11等のようなコンピュータにおけるメモリ（RAM；図示せず）に読み出し、そのプログラムを起動してやはり図示しないプロセッサ回路（カード型記憶媒体1内のMPU又は図2に示す端末11等のようなコンピュータにおけるCPU等）で実行することにより、プロセッサ回路の動作として実現される。

【0036】ここで、カード型記憶媒体用アクセス制御プログラムは、アクセス主体を識別するためのクリアランス情報9（照合用クリアランス情報9A、認証用クリアランス情報9B）を生成するクリアランス情報生成部5、アクセス主体からのアクセス要求先となるデータに対応して設定されたアクセス権限情報3-iを読み込むアクセス権限情報読込部6、および、上記クリアランス情報9及びアクセス権限情報3-iからクリアランス情報9に対応したアクセス権限を求め、求められたアクセス権限に基づいて、アクセス主体からのデータへのアクセスを制御する制御部7として、カード型記憶媒体1又はコンピュータを機能させるものである。

【0037】なお、このカード型記憶媒体用アクセス制御プログラムは、例えばCD-ROM等に記録されており、CD-ROM等から、カード型記憶媒体1内のROMに予め記憶されたり、図2に示す端末11等のようなコンピュータにおけるディスク装置等にインストールされて使用される。ここで、本実施形態にかかるカード型記憶媒体1のアクセス制御について、ある企業において、人事・経理部長及び経理課長がカード型記憶媒体1内に格納される人事情報にアクセスする場合を例にあげて説明する。

【0038】カード型記憶媒体1としてICカードを用いた場合のセキュリティシステムの構成例を図8

(a)、図8(b)に示す。ここで、人事・経理部長（符号Aで示す）は人事・経理部長の身分を示す暗証番号をもっており、経理課長（符号Bで示す）は経理課長の身分を示す暗証番号をもってしているものとする。

【0039】また、符号11AはICカード1Aに対して人事処理が可能な端末であり、符号11BはICカード1Bに対して経理処理が可能な端末である。さらに、符号10A、10Bは前述したカード接続装置である。

12

そして、ICカード1A、1Bは、前述した図3に示すような構成を有している。図3において、符号14はカード接続装置と命令の伝達／通知処理を行なう通信制御部、符号12は人事処理又は経理処理を行なうためのクライアントアプリケーション、符号4は前述したアクセス制御部、符号2-1、2-2はそれぞれ人事情報及び経理情報を格納するファイル、符号3-1、3-2はそれぞれファイル2-1における人事情報及びファイル2-2における経理情報に付与されたアクセス権限情報である。

【0040】なお、図8(a)、図8(b)に示す端末11A、11Bを用いて人事処理又は経理処理を行なう場合には、ICカード1A、1B内の人事情報及び経理情報に対して読み書き等のアクセスを行なおうとする主体（即ち、人事・経理部長A、経理課長B、端末11A、11B、実際にアクセスを行なうICカード1A、1B内のクライアントアプリケーション12又は図示しない端末11A、11B内のクライアントアプリケーション）を総称してアクセス主体という。

【0041】ここで、アクセス主体が人事情報又は経理情報に対してアクセスする際には、必ずアクセス制御部4を経由しなければならない構成をICカード1A、1Bはもっている。即ち、本実施形態では、ICカード1A、1Bは、図4に示すような構成をもっているのである。アクセス主体は、ICカード1A、1B内の人事情報又は経理情報に対して自分が正しいアクセス権限をもつことを示すために、図12に示すようなデフォルトのクリアランス情報（アクセス主体のデフォルトのクリアランス情報）をアクセス制御部4から獲得するように構成されている。なお、デフォルトのクリアランス情報には、認証用デフォルトクリアランス情報及び照合用デフォルトクリアランス情報の2種類があり、それぞれ、初期処理にてクリアランス情報の初期値としてロードされるものである。

【0042】本実施形態においては、アクセスする人物がアクセスが認められた人物であるかを照合するため、国際規格（ISO7816-4）における本人照合（Verify）コマンドが用いられる。また、アクセスする端末11A、11Bがアクセスが認められた端末であることを認証するため、国際規格（ISO7816-4）における外部認証（External Authenticate）コマンドが用いられる。

【0043】なお、本人照合コマンドにおける暗証番号、外部認証コマンドにおける暗号キー情報（認証キー情報）は、それぞれ照合用クリアランス情報9A及び認証用クリアランス情報9Bと連結している。さらに、本実施形態における照合により得られる照合用クリアランス情報を図13(a)、図13(b)に示し、本実施形態における認証により得られる認証用クリアランス情報を図14(a)、図14(b)に示す。なお、図13

50

(8)

13

(a) に示す照合用クリアランス情報9 A a 及び図1 4 (a) に示す認証用クリアランス情報9 B y は、人事・経理部長A に対応するものであり、図1 3 (b) に示す照合用クリアランス情報9 A b 及び図1 4 (b) に示す認証用クリアランス情報9 B z は、経理課長B に対応するものである。

【0044】また、前述したように、ICカード1 A, 1 B 内の人事情報及び経理情報には、クリアランス情報9 A, 9 B に対応したアクセス権限を生成するアクセス権限情報3-1, 3-2 がそれぞれ定義されている。ここで、図1 5 に人事情報に付与されるアクセス権限情報3-1 の一部を示し、図1 6 に経理情報に付与されるアクセス権限情報3-2 の一部を示す。

【0045】さらに、アクセス権限情報3-1, 3-2 としては、アクセス主体のアクセス権限を演算により求めるために、アクセス権限許可演算子F o 1, F o 2

〔図1 5, 図1 6 及び次式(2), (3) 参照] 及びアクセス権を許可する条件(アクセス権限要素f o 1 1 ~ f o 2 9; 図1 7, 図1 8 参照) が定義されている。なお、図1 7 に人事情報に付与されるアクセス権限情報3-1 の一部を示し、図1 8 に経理情報に付与されるアクセス権限情報3-2 の一部を示す。

【0046】

$$F o 1 = f o 1 1 + f o 1 4 + f o 1 7 \quad \cdots (2)$$

$$F o 2 = f o 2 2 + f o 2 5 + f o 2 8 \quad \cdots (3)$$

例えば、図1 7 に示す人事情報に付与されるアクセス権限情報3-1 では、アクセス権限要素f o 1 1 は「部長／人事(つまり人事部長)」のクリアランス情報をもつアクセス主体に対するアクセス権限が定義されている。

【0047】そして、アクセス権限情報3-1, 3-2 では、照合用クリアランス情報9 A 及び認証用クリアランス情報9 B をともに取得したアクセス主体に対しては、全てのアクセス権限(R: リード権, W: ライト権, X: 削除権) が許可されるように設定されている。また、照合用クリアランス情報9 A のみを取得したアクセス主体に対しては、リードのみが可能となり、その他は人事情報2-1 へのアクセスが認められないように設定されている。

【0048】そして、照合及び認証により獲得したアクセス主体のクリアランス情報9 A, 9 B は、そのアクセス主体のアクセスが閉塞されるまでアクセス制御部4 内で保持されるようになっている。なお、実際には、ICカード1 (1 A, 1 B) 内のデータは、図1 9 に示すような構造を有している。

【0049】この図1 9 は、ICカード1 内の不揮発性メモリの領域区分を示す図であり、前述した認証用デフォルトクリアランス情報及び照合用デフォルトクリアランス情報は、システム領域に格納されている。さらに、図1 9 に示すデータ域のファイル構成の詳細を図2 0 に示す。なお、図1 9, 図2 0 において、MF (Master F

14

ile) はDF (Dedicated File) の根幹となるものである。また、EF (Elementary File) としては、IEF (内部EF) とWEF (作業用EF) があり、IEF は認証用キーや照合用キー等やICカード1 内のクライアントアプリケーション以外のプログラムが管理・制御を目的として使用するデータを格納する領域であり、WEF はICカード1 内の各種プログラムではなく、外部機器(例えば端末1 1, 1 1 A, 1 1 B 等) が使用するデータを格納する領域である(なお、データ内容は外部機器により任意に定義される)。

【0050】なお、本実施形態にかかるカード型記憶媒体1 のアクセス制御について説明する際には、図2 1

(a), 図2 1 (b), 図2 2 (a) ~ 図2 2 (d), 図2 3 (a), 図2 3 (b) に示すファイル構成を前提とする。これらの図においては、説明上必要なものしかデータ内容を図示していない。上述のような構成により、本発明の一実施形態にかかるカード型記憶媒体1 においては、アクセス主体からカード型記憶媒体1 内のデータへのアクセス要求があると、アクセス制御部4 では、アクセス要求に対するアクセス制御が行なわれる。このとき、アクセス制御部4 においては、まず、クリアランス情報生成部5 により、アクセス主体から送信された暗証番号及び暗号キー情報(認証キー情報) に基づいて、アクセス主体を識別するためのクリアランス情報9 (照合用クリアランス情報9 A, 認証用クリアランス情報9 B) が生成される(クリアランス情報生成ステップ; 図3 7 のステップS 1)。

【0051】詳細には、クリアランス情報生成部5 では、アクセス主体からオペレータの身分を示す暗証番号及びアプリケーションを識別するための暗号キー情報が入力されると、入力された暗証番号及び暗号キー情報が参照用の暗証番号及び参照用の暗号キー情報と比較される。そして、一致した場合には、前述したクリアランス情報発生情報を用いて参照用の暗証番号及び参照用の暗号キー情報に対応した照合用クリアランス情報及び認証用クリアランス情報を発生し、前述した演算関数を用いて発生した照合用クリアランス情報及び認証用クリアランス情報がデフォルトの照合用クリアランス情報及びデフォルトの認証用クリアランス情報に反映されて(即ち、クリアランス情報が更新されて)、照合用クリアランス情報9 A 及び認証用クリアランス情報9 B が生成される。

【0052】なお、デフォルトのクリアランス情報の発生について、図3 1 を用いて説明すると、図3 1 に示すように、カード型記憶媒体(ICカード) 1 に電源が供給されると、カード型記憶媒体1 内のMPU 又は端末1 1 (1 1 A, 1 1 B) におけるCPU がリセットされ初期処理が開始される。そして、この初期処理において、アクセス制御部4 が前述したシステム領域から認証用デフォルトクリアランス情報及び照合用デフォルトクリア

10

20

30

40

50

(9)

15

ランス情報をロードすることにより、デフォルトのクリアランス情報が発生する。

【0053】さらに、クリアランス情報の更新について、図32～図34を用いて説明する。ここで、認証用クリアランス情報の更新について説明すると、図32に示すように、MFにて認証用キー（この認証用キーはIEF“1”の領域に格納されている）がロードされた場合には、デフォルトの認証用クリアランス情報が得られる。そして、認証用キーが正しければ、上記発生した認証用クリアランス情報に基づいて、認証用クリアランス情報が更新される。さらに、図33に示すように、DF“1”にて認証用キー（この認証用キーはIEF“3”の領域に格納されている）がロードされた場合には、更新された認証用クリアランス情報が得られる。そして、認証用キーが正しければ、上記発生した認証用クリアランス情報に基づいて、更に認証用クリアランス情報が更新される。

【0054】また、照合用クリアランス情報の更新について説明すると、MFにて照合用pin（照合用キー；この照合用キーはIEF“2”の領域に格納されている）がロードされると、デフォルトの照合用クリアランス情報が得られる。そして、照合用キーが正しければ、上記発生した照合用クリアランス情報に基づいて、照合用クリアランス情報が更新される（図34参照）。なお、照合用クリアランス情報が更新される様子を図9（a）～図9（c）にも示す。

【0055】続いて、アクセス制御部4においては、アクセス権限情報読込部6により、アクセス主体からのアクセス要求先となるデータに対応して設定されたアクセス権限情報3-iが読み込まれる（アクセス権限情報読込ステップ；図37のステップS2）。そして、制御部7により、上記クリアランス情報9及びアクセス権限情報3-iからクリアランス情報9に対応したアクセス権限が求められ、求められたアクセス権限に基づいて、アクセス主体からのデータへのアクセスが制御される（制御ステップ；図37のステップS3）。

【0056】詳細には、制御部7では、照合用クリアランス情報9A及び認証用クリアランス情報9Bを条件としてアクセス権限要素（例えば図17、図18に示すf011～f029）が決定され、アクセス権限要素を用いた演算により、クリアランス情報9に対応したアクセス権限が求められる。なお、アクセス権限の算出について、図35、図36を用いて説明すると、図35に示すように、クリアランス情報生成部5により生成された照合用クリアランス情報9A及び認証用クリアランス情報9Bに基づいて、WEF“1”の領域のレコードリードが行なわれ、アクセス権限要素が読みだされる。その後、アクセス権限要素を用いた演算により、クリアランス情報9に対応したアクセス権限が求められる（図36参照）。

16

【0057】さらに、実際のカード型記憶媒体1における動作を示すフローチャートを図38～図45に示す。図38は、カード型記憶媒体1における全体的な動作を示すフローチャートである。なお、図38に示すステップA1の詳細を図39に示し、図38に示すステップA4の詳細を図40に示す。また、図40に示すステップB4～B7の詳細をそれぞれ図41～図44に示し、図43に示すステップB19及び図44に示すステップB24の詳細を図45に示す。

【0058】カード型記憶媒体1においては、アクセス制御部4では、まず、クリアランス情報生成部5により、前述したシステム領域〔図19、図21（a）参照〕から認証用デフォルトクリアランス情報及び照合用デフォルトクリアランス情報がロードされて、デフォルトのクリアランス情報が発生する（図38のステップA1、図39のステップB1、B2）。

【0059】続いて、アクセス制御部4では、アクセス主体から各種コマンドが送信されたか（アクセス主体からの各種コマンドを受信したか）が判断され（図38のステップA2）、コマンドを受信しない場合にはコマンドを受信するまでこのステップA2の動作が繰り返される。また、コマンドを受信した場合には、アクセス制御部4では、コマンドを受信した順に監査ログ8（図2参照）の記録が行なわれる（図38のステップA3）。

【0060】そして、アクセス制御部4では、受信したコマンドに対する処理が行なわれる（図38のステップA4）。即ち、アクセス制御部4では、まず、受信したコマンドの種別が判断され（図40のステップB3）、コマンドの種別に応じた処理が行なわれる（図40のステップB4～B7）。つまり、受信したコマンドが本人照合コマンドである場合には本人照合コマンドに対する処理が行なわれ（図40のステップB4）、受信したコマンドが外部認証コマンドである場合には外部認証コマンドに対する処理が行なわれ（図40のステップB5）、受信したコマンドがリードレコードコマンドである場合にはリードレコードコマンドに対する処理が行なわれ（図40のステップB6）、受信したコマンドがライトレコードコマンドである場合にはライトレコードコマンドに対する処理が行なわれる（図40のステップB7）。

【0061】そして、受信したコマンドに対する処理を行なった後に、その処理に対してレスポンス応答し（図38のステップA5）、コマンドを処理した順に監査ログ8の記録が行なわれる（図38のステップA6）。ここで、図40のステップB4における本人照合コマンドに対する処理について、更に図41を用いて説明する。

【0062】受信したコマンドが本人照合コマンドである場合には、アクセス制御部4では、クリアランス情報生成部5により、前述したデータ域〔図19、図20、図21（b）参照〕のカレントDFにおける暗証番号

(10)

17

(pin)用のIEFに格納される暗証番号がロードされる(図41のステップB8)。そして、クリアランス情報生成部5では、本人照合コマンドとともに送信された暗証番号がロードされた暗証番号と同一かどうか判断され(図41のステップB9)、同一である場合には前述したようにして照合用クリアランス情報9Aを生成し(図41のステップB10)、“正常終了”というレスポンス情報が作成される(図41のステップB11)。また、送信された暗証番号がロードされた暗証番号と同一ではない場合には、“暗証番号照合エラー”というレスポンス情報が作成される(図41のステップB12)。

【0063】また、図40のステップB5における外部認証コマンドに対する処理について、更に図42を用いて説明する。受信したコマンドが外部認証コマンドである場合には、アクセス制御部4では、クリアランス情報生成部5により、前述したデータ域〔図19、図20、図21(b)参照〕のカレントDFにおける認証キー情報(キー)用のIEFに格納される認証キー情報がロードされ(図42のステップB13)、外部認証コマンドとともに送信された認証キー情報(入力データ)がロードキーを用いて復号される(図42のステップB14)。

【0064】そして、クリアランス情報生成部5では、ロードされた認証キー情報(平文)が復号された認証キー情報(復号文)と同一かどうか判断され(図42のステップB15)、同一である場合には前述したようにして認証用クリアランス情報9Bを生成し(図42のステップB16)、“正常終了”というレスポンス情報が作成される(図42のステップB17)。また、平文が復号文と同一ではない場合には、“キー認証エラー”というレスポンス情報が作成される(図42のステップB18)。

【0065】さらに、図40のステップB6におけるリードレコードコマンドに対する処理について、更に図43を用いて説明する。受信したコマンドがリードレコードコマンドである場合には、アクセス制御部4では、アクセス要求(リード要求)に対するアクセス制御が行なわれる。即ち、アクセス制御部4では、上述のごとく生成された照合用クリアランス情報9A、認証用クリアランス情報9Bと、アクセス権限情報読込部6により読み込まれたアクセス要求先となるデータに対応するアクセス権限情報3-iとに基づいて、制御部7によりアクセス権限の演算が行なわれる(図43のステップB19)。

【0066】そして、求められたアクセス権限ではリード権限が許可されているかが判断され(図43のステップB20)、リード権限が許可されている場合にはアクセス要求先となるデータ(該当レコード)が読み出され(図43のステップB21)、“正常終了”というレス

18

ポンス情報が作成される(図43のステップB22)。また、リード権限が許可されていない場合には、“セキュリティ異常”というレスポンス情報が作成される(図43のステップB23)。

【0067】また、図40のステップB7におけるライトレコードコマンドに対する処理について、更に図44を用いて説明する。受信したコマンドがライトレコードコマンドである場合には、アクセス制御部4では、アクセス要求(ライト要求)に対するアクセス制御が行なわれる。即ち、アクセス制御部4では、上述のごとく生成された照合用クリアランス情報9A、認証用クリアランス情報9Bと、アクセス権限情報読込部6により読み込まれたアクセス要求先となるデータに対応するアクセス権限情報3-iとに基づいて、制御部7によりアクセス権限の演算が行なわれる(図44のステップB24)。

【0068】そして、求められたアクセス権限ではライト権限が許可されているかが判断され(図44のステップB25)、ライト権限が許可されている場合にはアクセス要求先となるデータ(該当レコード)の書き込みが行なわれ(図44のステップB26)、“正常終了”というレスポンス情報が作成される(図44のステップB27)。また、ライト権限が許可されていない場合には、“セキュリティ異常”というレスポンス情報が作成される(図44のステップB28)。

【0069】最後に、図43のステップB19及び図44のステップB24におけるアクセス権限の演算処理について、更に図45を用いて説明する。アクセス制御部4の制御部7では、アクセス権限情報読込部6により、アクセス要求先となるデータに対応するアクセス権限情報(客体ラベル)3-iが読み込まれ(図45のステップB29)、演算対象となるラベル情報があるかが判断される(図45のステップB30)。ここで、演算対象となるラベル情報がある場合には、アクセス主体(客体)のアクセス権限情報が求められ(図45のステップB31)、上記ステップB30の動作が繰り返される。また、演算対象となるラベル情報がない場合には、照合用クリアランス情報9A、認証用クリアランス情報9B及びアクセス権限情報3-iとに基づいて、前述したようにしてアクセス権限の演算が行なわれる(図45のステップB32)。そして、求められたアクセス権限のアクセス種別が判断され(図45のステップB33)、アクセス要求コマンド(リードレコードコマンド又はライトレコードコマンド)に応じて、アクセスの許可又は禁止の制御が行なわれる。

【0070】なお、上述したクリアランス情報生成ステップ(図37のステップS1)は、図38に示すステップA1(即ち、図39に示すステップB1、B2)、図40に示すステップB4、B5(即ち、図41のステップB8~B12、図42のステップB13~B18)に相当する。また、上述したアクセス権限情報読込ステッ

(11)

19

プ(図37のステップS2)及び制御ステップ(図37のステップS3)は、図40に示すステップB6、B7(即ち、図43のステップB19~B23、図44のステップB24~B28、更には図45のステップB29~B33)に相当する。

【0071】さらに、本実施形態にかかるカード型記憶媒体1のアクセス制御について、ある企業において、人事・経理部長がカード型記憶媒体1内のファイル2-1、2-2に格納される人事情報、経理情報(図3参照)にアクセスする場合を例にあげて説明する。まず、人事・経理部長が人事情報へアクセスする場合について、以下の(1)~(3)にわけて説明する。

(1) 本人照合

図24に示すように、人事・経理部長Aが、図24では図示しない端末〔例えば図8(a)に示すような端末11A〕のキーボードを用いて暗証番号“a”を入力すると、端末はその暗証番号“a”をICカード1Aに本人照合コマンドを使用して送信する。

【0072】本人照合コマンドが送信されると、ICカード1A内のアクセス制御部(図24では図示せず)は、暗証番号“a”の照合を行ない、正しく照合できた場合には、照合用クリアランス情報9Aaを発生する。なお、図25では、人事部長及び経理部長であることを示すクリアランス情報が発生した様子を示している。

(2) 端末認証

次に、アクセスする際に用いた端末がアクセス可能な正しい端末であることを示すために、端末の認証(外部認

$$\text{アクセス権限} = (f011) \text{ or } (f014) \text{ or } (f017) \dots (4)$$

そして、このようなアクセス権限の演算により、アクセス制御部は、アクセス主体に対して「RWX」のアクセスを許可する(図29参照)。従って、人事・経理部長はカード型記憶媒体1内に格納される人事情報にアクセスすることができる。例えば、人事情報の読み込みを行なう場合には、図4に示すリード処理は正しく実行され、アクセス主体は人事情報の読み込みを行なうことができる。

【0076】さらに、人事・経理部長が経理情報へアクセスする場合について説明する。上記(1)において、※

$$\text{アクセス権限} = (f022) \text{ or } (f025) \text{ or } (f028) \dots (5)$$

そして、このようなアクセス権限の演算により、アクセス制御部は、アクセス主体に対して「R-」のアクセスを許可する(図30参照)。従って、人事・経理部長はカード型記憶媒体1内に格納される経理情報に対して読み込みアクセスのみ行なうことができる。例えば、経理情報の読み込みを行なう場合には、図4に示すリード処理は正しく実行され、アクセス主体は経理情報の読み込みを行なうことができる。しかし、経理情報の書き込みを行なおうとする場合には、アクセス権限がないためアクセス制御部により書き込み処理が拒絶され、アクセス主体にエラーが通知される。

20

*証)が外部認証コマンドを使用して行なわれる。図26では、端末11Aは、暗号鍵(暗号キー情報)“y”により認証データを署名してICカード1Aに送信している。

【0073】外部認証コマンドが送信されると、ICカード1A内のアクセス制御部(図26では図示せず)

は、署名データが正しく復元できたかを判断することにより、端末11Aの認証を行なう(暗号鍵“y”による認証)。そして、正しく認証が行なえた場合には、認証用クリアランス情報9Byを発生する。なお、図27では、人事用端末であることを示すクリアランス情報が発生した様子を示している。

(3) 人事情報へのアクセス

上記で発生した照合用クリアランス情報9Aa、認証用クリアランス情報9Byをもつアクセス主体(人事・経理部長A)が、人事情報へのアクセスを試みる。アクセスする際に行なうアクセス制御部内のアクセス権限の演算を以下に示す。

【0074】照合及び認証で得られた各クリアランス情報9Aa、9Byをまとめて仮想的に表現すると図28に示すようになる。上記のアクセス主体がもつクリアランス情報9Aa、9Byに対して、アクセス対象の人事情報に付与されるアクセス権限情報3-1(図3参照)は、図29に示すように、アクセス権限要素f011、f014、f017の論理和演算子を有している。即ち、アクセス権限は次式(4)にて求められる。

【0075】

※図28に示すようなクリアランス情報9Aa、9Byを取得したときに、経理情報にアクセスする場合には、図30に示すようなアクセス権限の演算が行なわれる。図28に示すアクセス主体(人事・経理部長)がもつクリアランス情報9Aa、9Byに対して、アクセス対象の経理情報に付与されるアクセス権限情報3-2(図3参照)は、図30に示すように、アクセス権限要素f022、f025、f028の論理和演算子を有している。即ち、アクセス権限は次式(5)にて求められる。

【0077】

【0078】このように、本発明の一実施形態にかかるカード型記憶媒体1によれば、アクセス主体からカード型記憶媒体1内のデータへのアクセスを制御するアクセス制御部4をそなえることにより、多目的利用を考えた場合であっても、アクセス権限の設定、変更作業を簡素化しながら、セキュリティシステムの管理、運営を確実に行なうことができる。

【0079】つまり、カード型記憶媒体1内のデータに対するアクセス権限の設定、変更を行なう場合には、データに付与されるアクセス権限情報3-iにおけるアクセス権限を求めるための関数を変更するだけでよい

(12)

21

め、アクセス権限の設定、変更作業を簡素化することができる。また、アクセス主体からの全てのアクセス要求に対して、アクセス主体毎にクリアランス情報9を付与することができるので、セキュリティの監査をクリアランス情報9に基づいて確実に実施することができ、セキュリティシステムの性能を向上させることができる。従って、セキュリティシステムの管理、運営を確実にこなうことができる。

【0080】さらに、多目的利用を考えた場合でも、関連するクリアランス情報9とアクセス権限情報3-iだけに着目してセキュリティシステムを設計することができるので、複数のデータの独立性を保つことができる。なお、クリアランス情報9に対する演算を可能とすることにより、業務目的単位にクリアランス情報9を設けることができる。従って、例えばある業務から他の業務に変更するとき、ある業務で獲得したクリアランス情報9を削除することが可能となり、業務間でのクリアランス情報9の干渉を防ぐことができる。また、逆に業務間でクリアランス情報9を干渉させるように設定することもできる。

【0081】(b) その他

上述した一実施形態にかかるカード型記憶媒体1においては、クライアントアプリケーション12とアクセス制御部4との間に、アクセス主体からデータにアクセスするための論理チャネル13が1つだけ設けられている場合について説明したが、これに限定されず、図6に示すように、複数のクライアントアプリケーション12A、12Bとアクセス制御部4との間に論理チャネル13-1、13-2を複数設けることもできる。また、図示はしないが、1つのクライアントアプリケーションとアクセス制御部4との間に論理チャネル13-1、13-2を複数設けることもできる（即ち、図6に示すクライアントアプリケーション12A、12Bが同一のものである場合に相当する）。

【0082】これらの場合には、アクセス制御部4は、クライアントアプリケーション12A、12Bからデータへのアクセスを、論理チャネル13-1、13-2毎に独立して制御する。なお、この際には、アクセス制御部4は、論理チャネル13-1、13-2毎にクリアランス情報15a、15bを生成する。

【0083】

【発明の効果】以上詳述したように、請求項1～14記載の本発明によれば、多目的利用を考えた場合であっても、アクセス権限の設定、変更作業を簡素化しながら、セキュリティシステムの管理、運営を確実にこなうことができる利点がある。

【図面の簡単な説明】

【図1】本発明の一実施形態にかかるカード型記憶媒体の構成を示す機能ブロック図である。

【図2】本発明の一実施形態にかかるカード型記憶媒体

22

の構成を示す機能ブロック図である。

【図3】本発明の一実施形態にかかるカード型記憶媒体の構成を示す機能ブロック図である。

【図4】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するための図である。

【図5】クリアランス情報について説明するための図である。

【図6】複数のクライアントアプリケーションとアクセス制御部との間に論理チャネルが複数設けられた様子を示す図である。

【図7】監査ログの一例を示す図である。

【図8】(a)、(b)は、それぞれカード型記憶媒体としてICカードを用いた場合のセキュリティシステムの構成例を示す図である。

【図9】(a)～(c)は、それぞれ照合用クリアランス情報が更新される様子を示す図である。

【図10】(a)～(c)は、それぞれクリアランス情報について説明するための図である。

【図11】アクセス権限情報について説明するための図である。

【図12】デフォルトのクリアランス情報を示す図である。

【図13】(a)、(b)は、それぞれ照合用クリアランス情報を示す図である。

【図14】(a)、(b)は、それぞれ認証用クリアランス情報を示す図である。

【図15】人事情報に付与されるアクセス権限情報を示す図である。

【図16】経理情報に付与されるアクセス権限情報を示す図である。

【図17】アクセス権の条件定義を示す図である。

【図18】アクセス権の条件定義を示す図である。

【図19】ICカード内の不揮発性メモリの領域区分を示す図である。

【図20】図19に示すデータ域のファイル構成の詳細を示す図である。

【図21】(a)、(b)は、それぞれICカード内の不揮発性メモリにおけるファイル構成を示す図である。

【図22】(a)～(d)は、それぞれ図21に示すファイル構成の詳細を示す図である。

【図23】(a)、(b)は、それぞれ図21に示すファイル構成の詳細を示す図である。

【図24】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するための図である。

【図25】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するための図である。

【図26】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するための図である。

【図27】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するための図である。

(13)

23

【図28】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するための図である。

【図29】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するための図である。

【図30】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するための図である。

【図31】デフォルトのクリアランス情報の発生について説明するための図である。

【図32】クリアランス情報の更新について説明するための図である。

【図33】クリアランス情報の更新について説明するための図である。

【図34】クリアランス情報の更新について説明するための図である。

【図35】アクセス権限の算出について説明するための図である。

【図36】アクセス権限の算出について説明するための図である。

【図37】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するためのフローチャートである。

【図38】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するためのフローチャートである。

【図39】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するためのフローチャートである。

【図40】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するためのフローチャートである。

【図41】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するためのフローチャートである。

【図42】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するためのフローチャートである。

【図43】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するためのフローチャートである。

24

【図44】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するためのフローチャートである。

【図45】本発明の一実施形態にかかるカード型記憶媒体の動作を説明するためのフローチャートである。

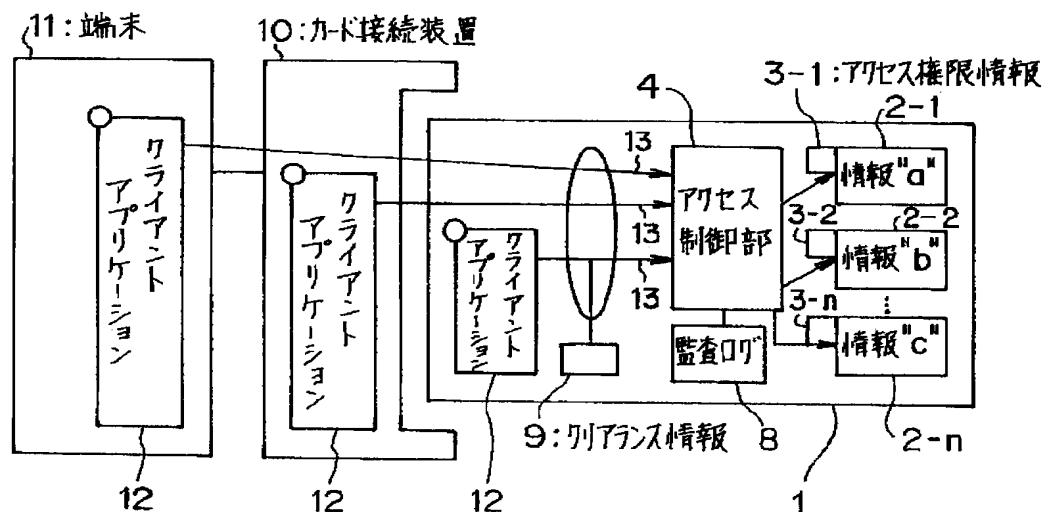
【図46】(a), (b)は、それぞれ従来のカード型記憶媒体におけるアクセス制御方法について説明するための図である。

【図47】従来のカード型記憶媒体におけるアクセス制御方法について説明するための図である。

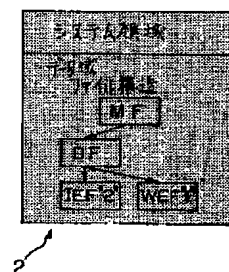
10 【符号の説明】

- 1, 1A, 1B カード型記憶媒体 (ICカード)
- 2-1~2-n ファイル (記憶部)
- 3-1~3-n アクセス権限情報
- 4 アクセス制御部
- 5 クリアランス情報生成部 (アクセス主体識別情報生成部)
- 6 アクセス権限情報読込部
- 7 制御部
- 8 監査ログ
- 9, 15a, 15b クリアランス情報
- 9A, 9Aa, 9Ab 照合用クリアランス情報
- 9B, 9By, 9Bz 認証用クリアランス情報
- 10, 10A, 10B カード接続装置
- 11, 11A, 11B 端末 (外部機器)
- 12, 12A, 12B クライアントアプリケーション
- 13, 13-1, 13-2 論理チャンネル
- 14 通信制御部
- 100 ICカード
- 101-1, 101-2 ファイル
- 102-1, 102-2, 102-1', 102-1''
アクセス権限情報
- 103A~103D クライアント

【図2】

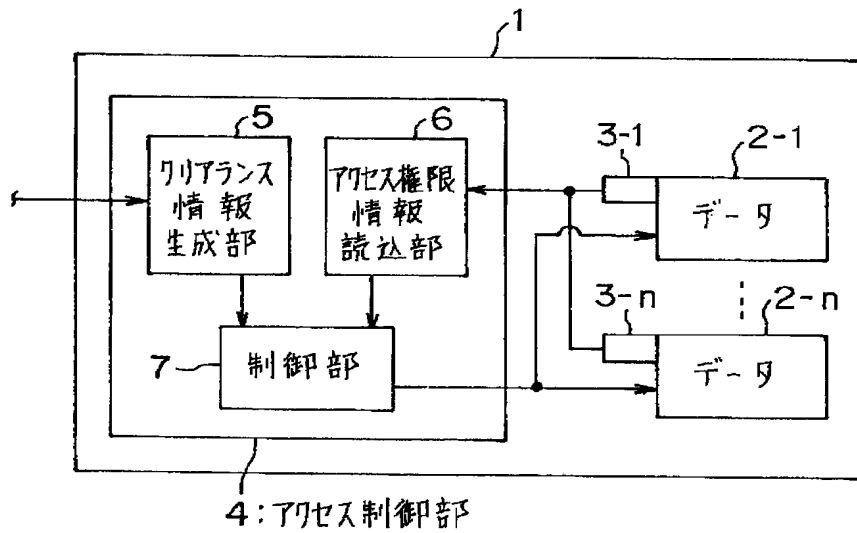


【図19】



(14)

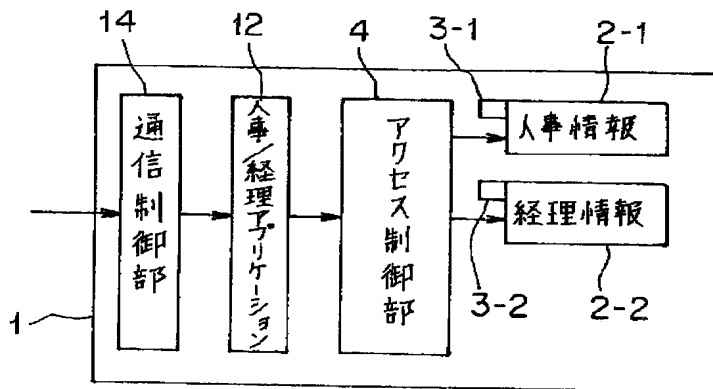
【図1】



【図12】

リアランス情報		カテゴリ		
		人事	経理	その他
レベル	部長			
	課長			
	その他			

【図3】



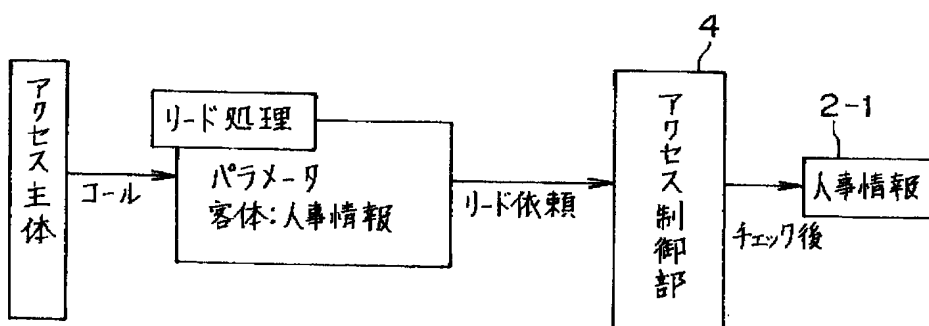
【図15】

演算子: Fo1		カテゴリ		
人事情報ラベル情報		人事	経理	その他
レベル	部長	fo11	fo12	fo13
	課長	fo14	fo15	fo16
	その他	fo17	fo18	fo19

【図16】

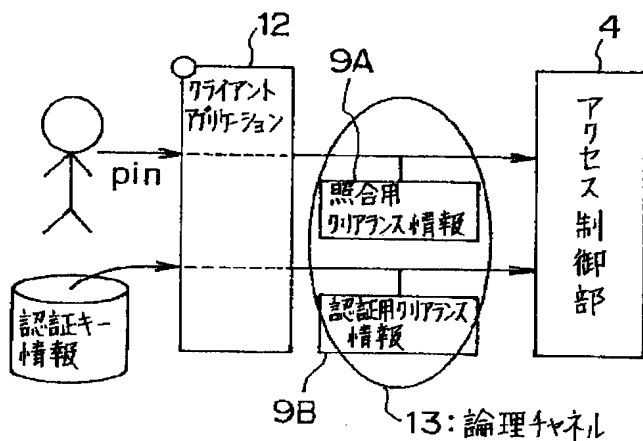
演算子: Fo2		カテゴリ		
経理情報ラベル情報		人事	経理	その他
レベル	部長	fo21	fo22	fo23
	課長	fo24	fo25	fo26
	その他	fo27	fo28	fo29

【図4】



(15)

【図5】



【図10】

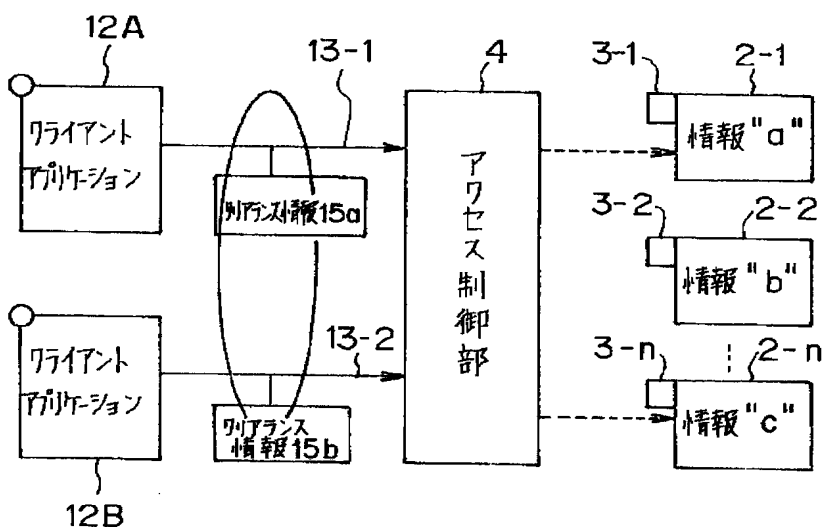
(a)

照合用リソース情報		カテゴリ				
		人事	経理	総務	開発	購買
レベル	部長		○			
	担当部長			○		
	課長		○			
	一般職					

(b)

認証用リソース情報		カテゴリ				
		人事	経理	総務	開発	購買
レベル	部長					
	担当部長			○		○
	課長		○			
	一般職					

【図6】



(c)

照合/認証用リソース情報		カテゴリ				
		人事	経理	総務	開発	購買
レベル	部長		○			
	担当部長			○		-○
	課長		○			
	一般職					

【図25】

照合用リソース情報 9Aa		カテゴリ		
		人事	経理	その他
レベル	部長	○	○	
	課長			
	その他			

【図13】

【図14】

(a)					(b)					(a)					(b)				
照合(暗証番号"a":人事・経理部長)					照合(暗証番号"b":経理課長)					認証(暗証番号"y":人事端末)					認証(暗証番号"z":経理端末)				
照合用リソース情報 9Aa		カテゴリ			照合用リソース情報 9Ab		カテゴリ			認証用リソース情報 9By		カテゴリ			認証用リソース情報 9Bz		カテゴリ		
レベル	部長	課長	その他	その他	レベル	部長	課長	その他	その他	レベル	部長	課長	その他	その他	レベル	部長	課長	その他	その他
	○	○									○					○			
							○				○					○			
											○						○		

(16)

【図7】

監査ログファイル(IEF)

コード No	レコード
1	コマンド受信 (1回目)
2	コマンド結果 (1回目)
3	コマンド受信 (2回目)
4	コマンド結果 (2回目)
5	コマンド受信 (3回目)
...	...
n	コマンド結果 (m回目)

コマンド受信情報は、コマンド受信ごとにカウントする。
 コマンド結果情報は、コマンド結果ごとにカウントする。
 コマンド受信情報は、コマンド受信ごとにカウントする。
 コマンド結果情報は、コマンド結果ごとにカウントする。
 コマンド受信情報は、コマンド受信ごとにカウントする。
 コマンド結果情報は、コマンド結果ごとにカウントする。
 コマンド受信情報は、コマンド受信ごとにカウントする。
 コマンド結果情報は、コマンド結果ごとにカウントする。

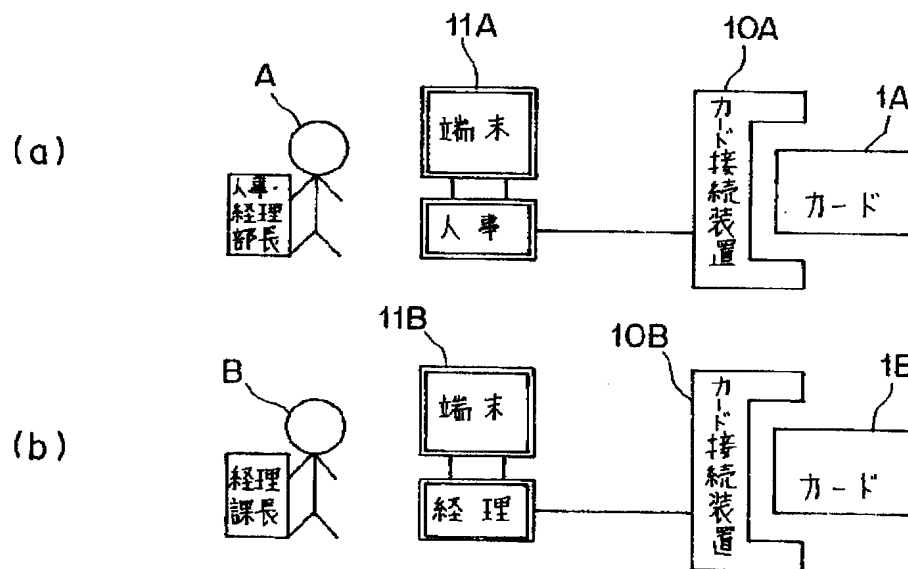
【図17】

アクセス権の条件定義 R:リード権 W:ライト権 X:削除権

fo11: 照合 認証 Tアクセス権 ○ ○ =RWX ○ ○ =R-- -- ○ =--- -- -- =---	fo12: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---	fo13: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---
fo14: 照合 認証 Tアクセス権 ○ ○ =RW-- ○ ○ =R-- -- ○ =--- -- -- =---	fo15: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---	fo16: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---
fo17: 照合 認証 Tアクセス権 ○ ○ =R-- ○ ○ =--- -- ○ =--- -- -- =---	fo18: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---	fo19: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---

【図26】

【図8】



【図18】

【図21】

【図27】

認証用 クリアランス 情報 9By	カテゴリ		
	人事	経理	その他
部長	○		
課長	○		
その他	○		

アクセス権の条件定義 R:リード権 W:ライト権 X:削除権

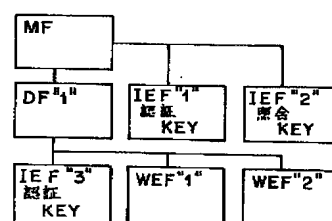
(a)

(b)

fo21: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---	fo22: 照合 認証 Tアクセス権 ○ ○ =RWX ○ ○ =R-- -- ○ =--- -- -- =---	fo23: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---
fo24: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---	fo25: 照合 認証 Tアクセス権 ○ ○ =RW- ○ ○ =R-- -- ○ =--- -- -- =---	fo26: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---
fo27: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---	fo28: 照合 認証 Tアクセス権 ○ ○ =R-- ○ ○ =--- -- ○ =--- -- -- =---	fo29: (未定義) 照合 認証 Tアクセス権 ○ ○ =--- ○ ○ =--- -- ○ =--- -- -- =---

システム領域

認証用 クリアランス情報 9By
人事
経理
その他



(17)

【図9】

(a) 経理部長兼経理課長のリライアンスを持っている。

リライアンス情報		カテゴリ				
		人事	経理	総務	開発	購買
レベル	部長		○			
	担当部長					
	課長		○			
	一般職					

(b) 新たに総務担当部長のリライアンスを取得。

リライアンス情報		カテゴリ				
		人事	経理	総務	開発	購買
レベル	部長					
	担当部長			○		
	課長					
	一般職					

(c) リライアンスの演算関数を用いた情報の論理和定義の場合。

リライアンス情報		カテゴリ				
		人事	経理	総務	開発	購買
レベル	部長		○			
	担当部長			○		
	課長		○			
	一般職					

【図11】

アクセス権限情報

Fo:結合論理関数

認証用リライアンス情報		カテゴリ				
		人事	経理	総務	開発	購買
レベル	部長	fo11	fo12	fo13	fo14	fo15
	担当部長	fo21	fo22	fo23	fo24	fo25
	課長	fo31	fo32	fo33	fo34	fo35
	一般職	fo41	fo42	fo43	fo44	fo45

fo12:照合 認証 7桁以降
○ ○ =RWX
○ ○ =RW-
- ○ =R-
- - =-

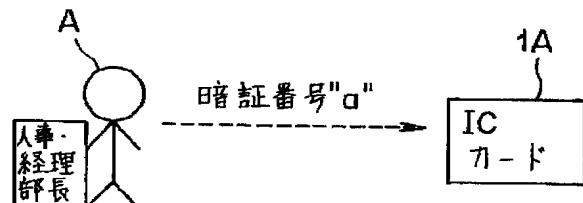
fo23:照合 認証 7桁以降
○ ○ =RWX
○ ○ =RW-
- ○ =R-
- - =-

fo25:照合 認証 7桁以降
○ ○ =RWX
○ ○ =RW-
- ○ =R-
- - =-

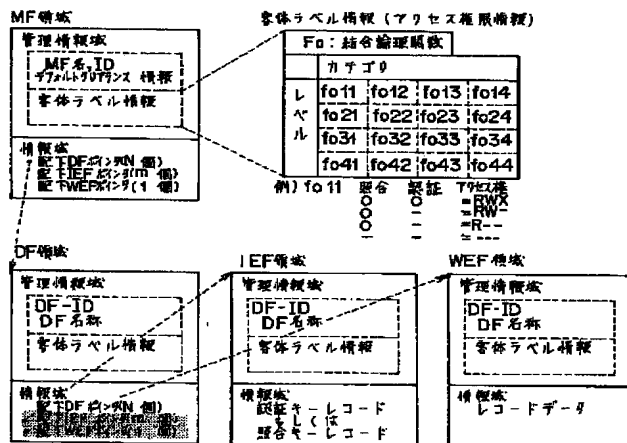
fo32:照合 認証 7桁以降
○ ○ =RWX
○ ○ =RW-
- ○ =R-
- - =-

Fo = (fo12 or fo23) and (fo32) - (1)の場合に得られるアクセス権は、
Fo = (RW- or RW-) and (RWX)
= RW-

【図24】



【図20】



【図28】

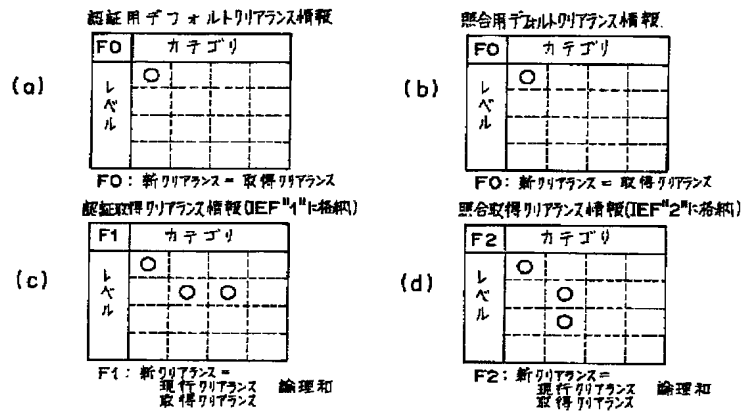
照合用リライアンス情報 9Aa		カテゴリ		
		人事	経理	その他
レベル	部長	○	○	
	課長			
	その他			

認証用リライアンス情報 9By		カテゴリ		
		人事	経理	その他
レベル	部長	○		
	課長	○		
	その他	○		

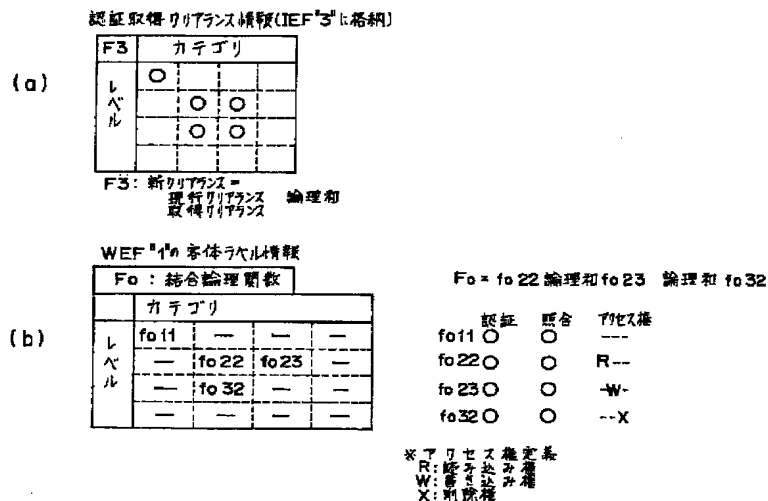
照合・認証用リライアンス情報 9		カテゴリ		
		人事	経理	その他
レベル	部長	○	○	
	課長	○		
	その他	○		

(18)

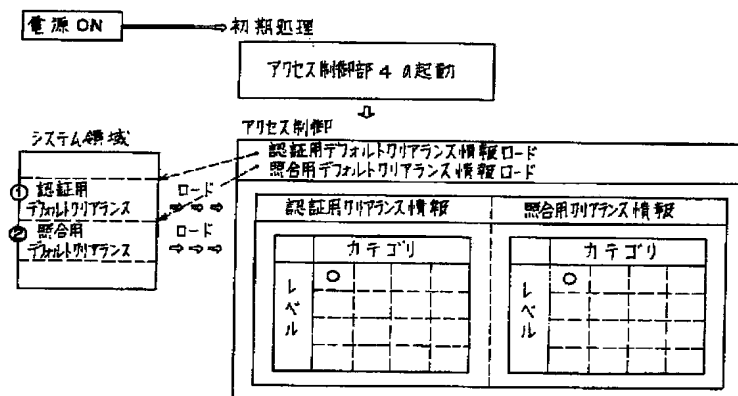
【図22】



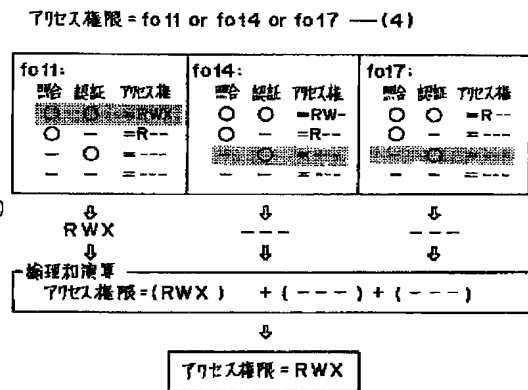
【図23】



【図31】

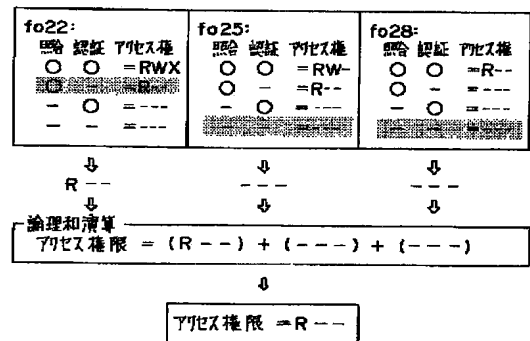


【図29】

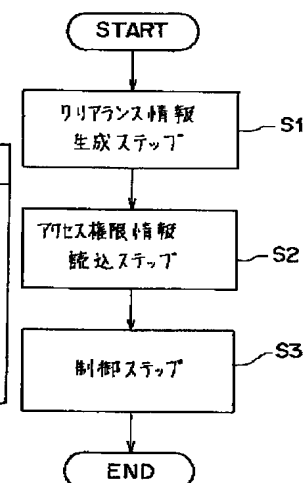


【図30】

リソース権限 = fo22 or fo25 or fo28 — (5)

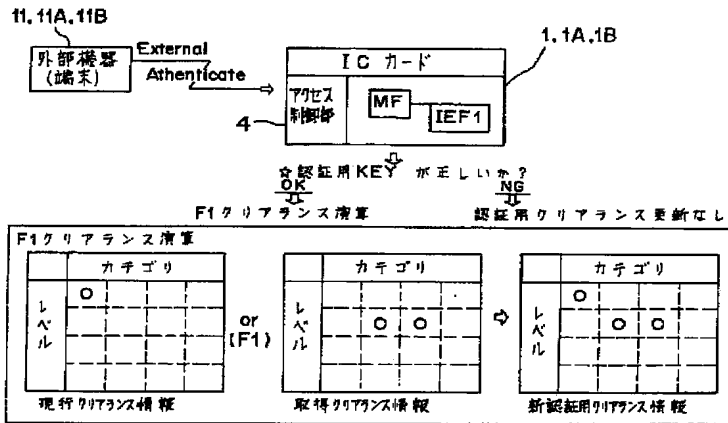


【図37】

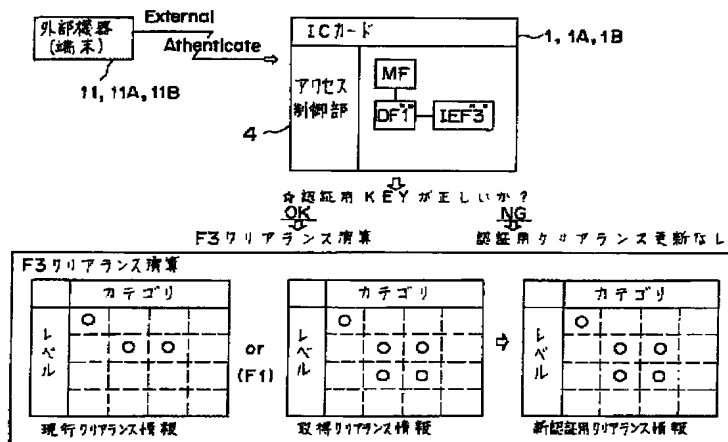


(19)

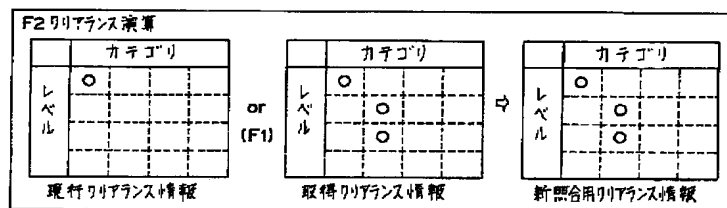
【図32】



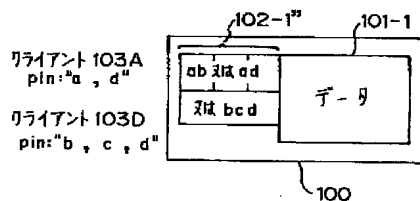
【図33】



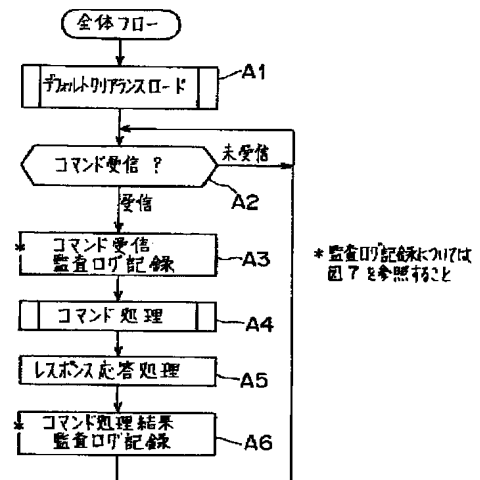
【図34】



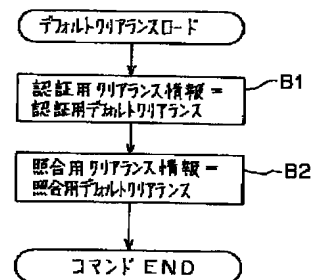
【図47】



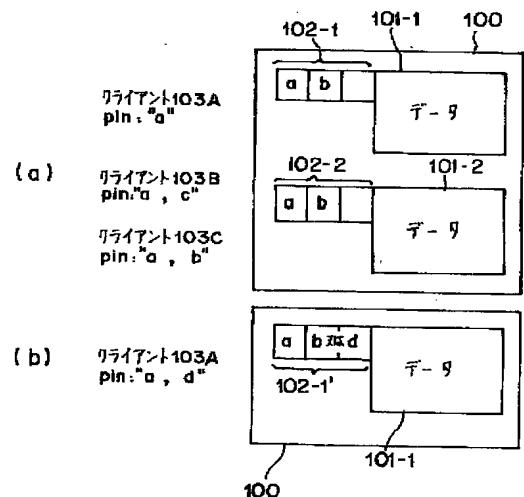
【図38】



【図39】

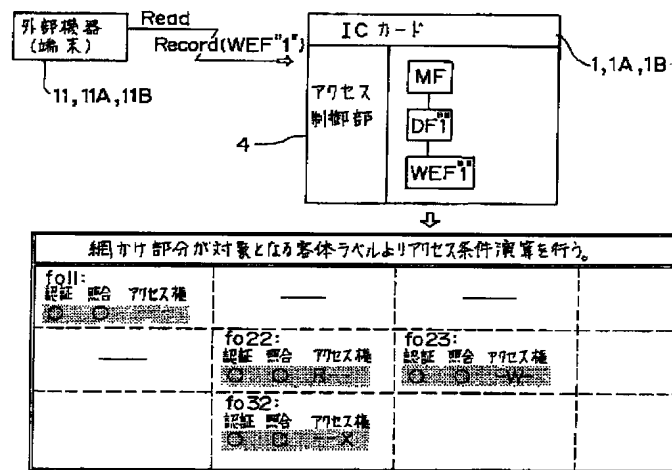


【図46】

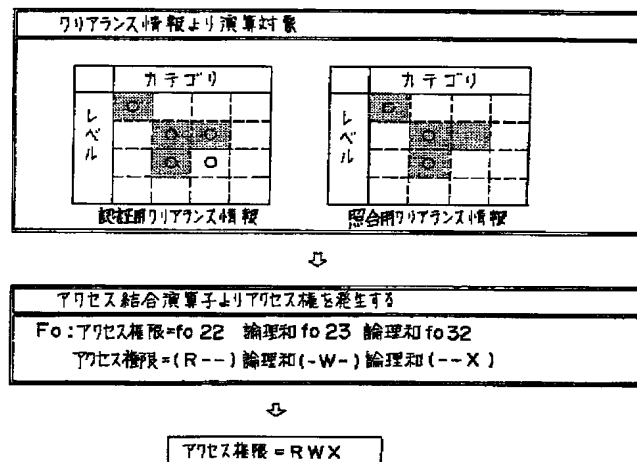


(20)

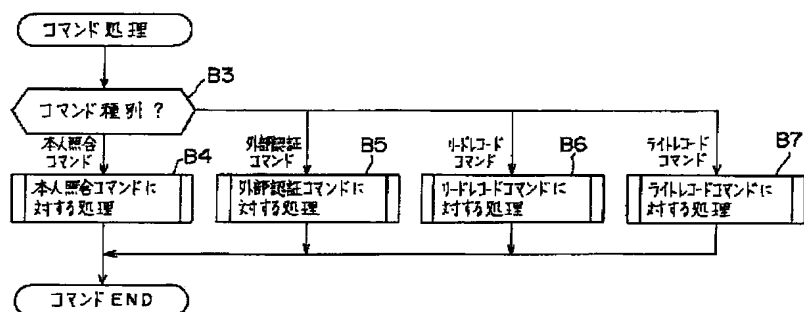
【図35】



【図36】

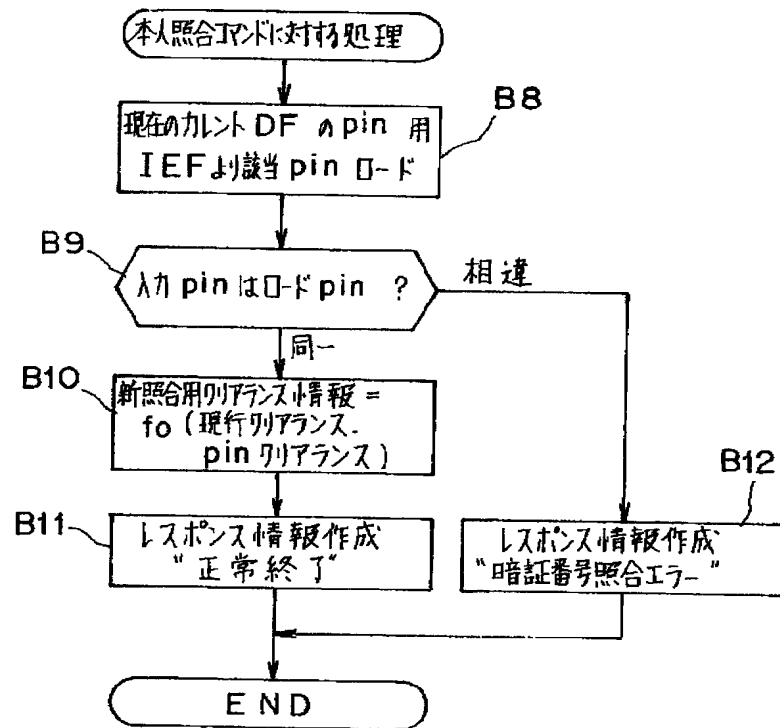


【図40】

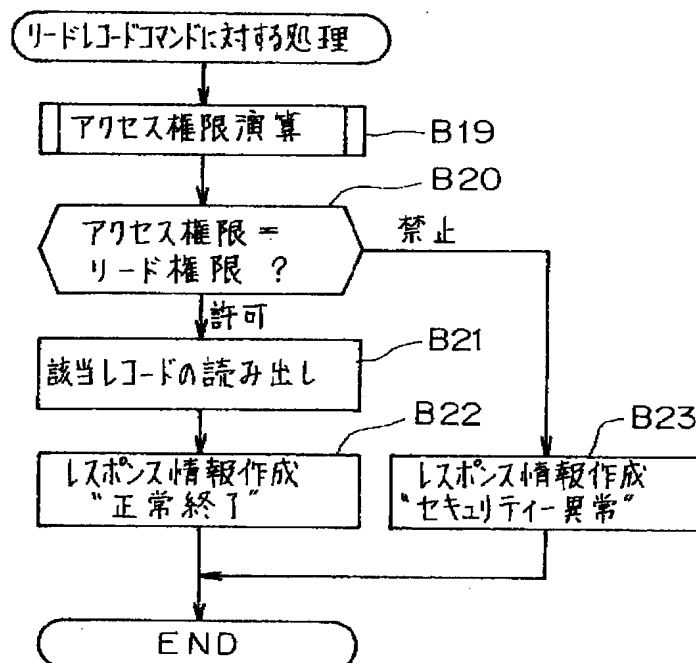


(21)

【図41】

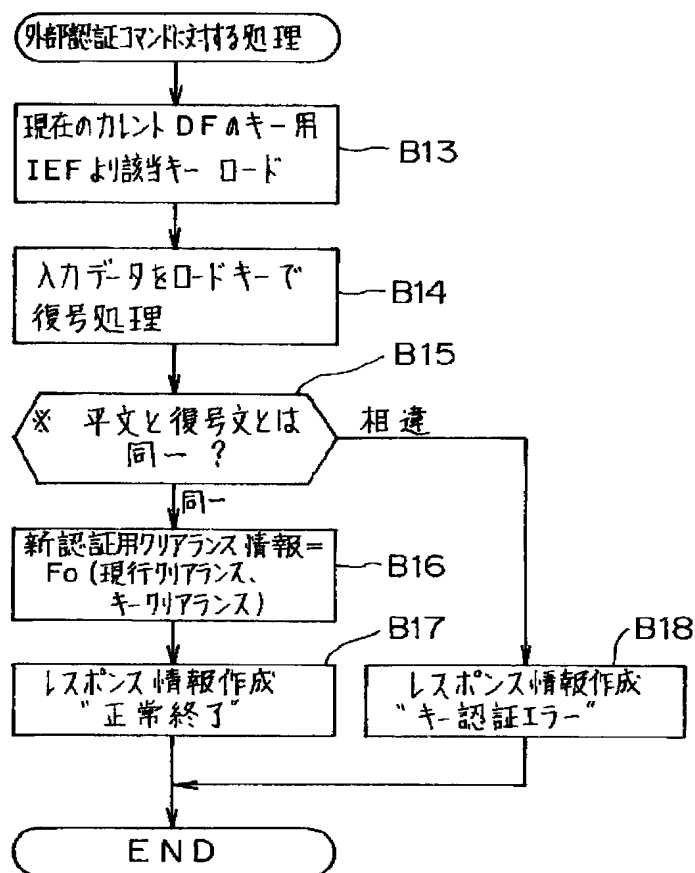


【図43】



(22)

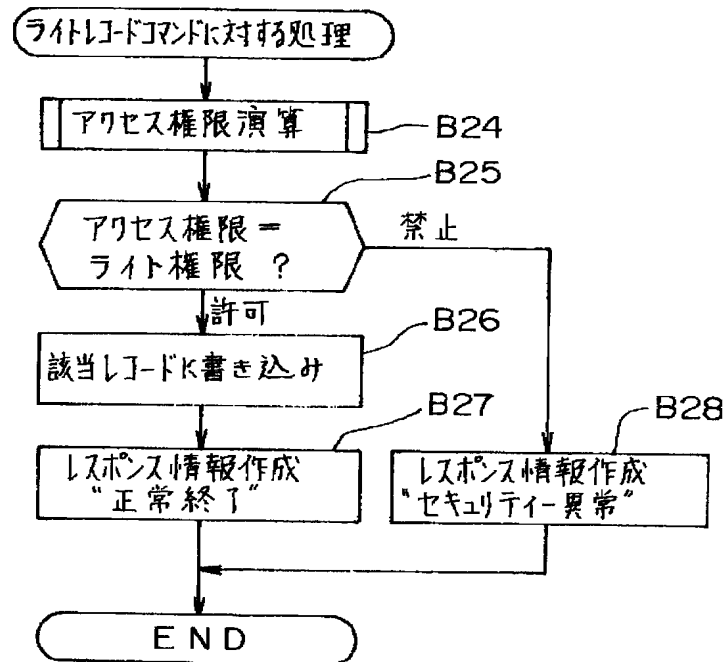
【図42】



※ External コマンドの前には IC カード内に
認証用データを保持していること。

(23)

【図44】



(24)

【図45】

